



The Digital ID Pipeline: *Understanding Age Verification Policies*

Why Age-Verification Mandates Lead to Digital ID Systems, Data Risks, and Expanded Government Power

Introduction

Across the country, lawmakers are advancing age-verification (AV) bills with the stated goal of protecting children online. These proposals are often framed as simple, common-sense measures: keep minors away from explicit content, empower parents, and hold platforms accountable. On the surface, it sounds straightforward. But the reality is far more complex. To verify someone's age online, a system must first verify who that person is. That means collecting, scanning, or matching identity-linked information, whether through a driver's license, a selfie, a phone number, a credit card, or a biometric scan. In practice, age verification is not a digital "lock on the liquor cabinet." It is the creation of an identity checkpoint for everyday internet use.

What's emerging is not just a child-safety tool, but the early architecture of a Digital ID system in the United States. Major think tanks, advocacy groups, and technology vendors now openly describe AV as a gateway to device-level identity signals, interoperable verification across apps and browsers, and government-mandated standards for how platforms confirm who is an adult and who is a minor. For the average person, this means that accessing websites, apps, or online

services could increasingly require proving your identity to a third-party verifier or to your device itself. The debate may be framed around protecting children, but the long-term consequence is the normalization of identity-gated access to the internet, an expansion of data collection, surveillance potential, and government authority that reaches far beyond the issue of online safety.



Top Five Arguments Used to Support Age Verification and Why They Fail

Age verification protects children from harmful content

This is the emotional centerpiece of every AV campaign. Supporters argue that children are exposed to extreme content and that age verification is the only way to stop it.

The Reality

Protecting children is important, but age-verification laws do not reduce exposure. Evidence from the UK, France, Utah, Texas, and Louisiana shows:

- Children simply switch to VPNs, foreign sites, or social media platforms that AV laws do not cover.
- Exposure does not decrease; it shifts to unmoderated, unregulated environments.
- The UK Children's Commissioner found no significant reduction in minors accessing pornography after AV rollout.

Age verification creates a false sense of safety while pushing children toward more dangerous corners of the internet.

Age verification can be done without collecting personal data

Organizations such as AVPA, Heritage Foundation, and EPPC all repeat this claim. They point to “zero-knowledge proofs,” “anonymous tokens,” or “privacy-preserving” systems.

The Reality

This is the most misleading claim in the debate.

Even so-called “anonymous” systems require identity-linked data such as:

- device fingerprints

- IP addresses
- metadata
- selfies
- facial scans
- phone numbers
- email addresses
- government ID scans
- database checks
- behavioral biometrics

These data points can be breached, subpoenaed, logged, or repurposed. There is no such thing as age verification without identity verification.

Third-party verifiers solve the privacy problem.

Supporters argue that if platforms never see your identity, privacy is protected.

The Reality

This simply outsources the Digital ID problem. It does not eliminate it.

Third-party verifiers become centralized identity hubs holding:

- biometric templates
- device fingerprints
- verification logs
- metadata
- behavioral data

These hubs are hackable, subpoena-able, and permanent. This is the architecture of a Digital ID system, just privatized.

The Supreme Court upheld Texas' age-verification law

This claim is used to suggest that AV laws are now constitutionally safe.

The Reality

This is inaccurate.

- The Supreme Court did not uphold the entire law.
- It allowed a narrow portion to take effect temporarily while litigation continues.
- Multiple federal courts have struck down similar laws.
- State constitutions have different privacy protections from state to state.

Constitutional risk is extremely high.

America should build a device-level age verification system

EPPC's "American Style Age Verification" **report** lays out a detailed plan for device-level identity checks at setup, with interoperable age signals shared across apps, browsers, and platforms.

The Reality

This is the clearest blueprint for a national Digital ID system we have seen.

EPPC explicitly calls for:

- device-level age verification
- operating-system-level age signals
- interoperability across apps and websites
- mandatory participation by Apple, Google, and Microsoft
- digital driver's licenses
- biometric verification
- credit-card-based age checks
- mobile-carrier age checks

Once device-level identity is mandated, every app, website, and browser becomes tied to a single identity credential. This is not about pornography. This is about identity-gating the entire internet.



Why Is the Most Conservative Think Tank Pushing for More Government?

This is a question every conservative should be asking.

The Heritage Foundation has historically championed limited government, individual liberty, and skepticism of centralized power.

Yet their AV **proposal** calls for:

- federal mandates
- device-level identity systems
- interoperability requirements
- government-approved verification providers
- nationwide technical standards
- expanded regulatory authority over Big Tech
- mandatory identity checks for online access

This is a dramatic expansion of government power over digital life.

Heritage argues that this is necessary to protect children. But the infrastructure they propose is identical to the Digital ID systems used in Europe, Australia, and Canada — systems conservatives have long opposed.

If the most conservative think tank in America is now advocating for a national identity-verification regime, we should be asking why.

Conclusion

Supporters of age-verification laws rely on five core arguments: child protection, privacy-preserving technology, third-party verifiers, constitutional safety, and the promise of an “American-style” system. But each of these claims collapses under scrutiny.

Age verification does not reduce exposure. It requires identity. It centralizes data. It expands government power. And it lays the groundwork for a Digital ID system that can be expanded far beyond pornography.

This debate is not about protecting children. It is about who controls identity, access, and speech in the digital age.

Support Our Mission

Conservative Ladies of America is a 501(c)(4) nonprofit working to stop unconstitutional age-verification mandates and defend the constitutional rights and data privacy of every American. As lawmakers push digital-ID-style policies that expand government power, we’re committed to exposing the truth and equipping citizens to stand up for their freedoms.

Your support helps us continue this critical work. Please consider making a one-time or monthly donation. Thank you for standing with us.

[Make A Donation](#)



Copyright © 2022. All Rights Reserved.



Copyright © 2022. All Rights Reserved.

